Published and Copyright (c) 1999 - 2015
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1746 12/11/15

~ DNS Root Servers Hack! ~ People Are Talking! ~ Firebee Update News!
~ COPPA Keeps Kids Safe? ~ HTTPS Encryption Suit! ~ ISIS Trolling Day!
~ FF7 Remake Episodes! ~ MS Security Bulletins! ~ PC Sales Falling?

-* France Looking at Tor, WiFi *-
-* Sony Unlocks PS4's Seventh CPU Core *-
-* Konami Bans Kojima From Game Awards Show! *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

There's a reason why I despise talking religion and politics, and a bigger one as to discussing a combination of the two!! Everyone has his own opinion, and neither is necessarily wrong.

Last week, I briefly mentioned Obama's lame speech from the Oval Office with regard to the terrorist attack in California. All that came out of his mouth was pure BS. One came away from listening to him, and scratching your head with the conclusion of "what was all that about?" Just more of the same Obama rhetoric that we've been listening to for years.

Love him or hate him, right or wrong - you have to give Donald Trump some credit for having the cajones to speak his mind. I don't agree with everything that he has to say, but it's obvious that he's not pussy-footing around. Forget political-correctness for the moment - there are a number of major issues in today's world that need attention. Toes are going to get stepped on. Some people's feelings are going to get hurt. Things are still interesting in the world of politics!

Until next time...

=~=~=~=

FireBee Update (Sort of)

By Fred Horvat

Well folks it's been a few weeks since my last FireBee installment. Besides the holidays and work I have been spending most of my free time getting my main computer back up to speed again which for now is done. Next installment I will be back where I left off with working further to find out why my FireBee does not want to run supported software on it. I did the Firmware and TOS upgrades but no luck with that helping. It doesn't hurt to be up to date so it was not a waste of time. I can just cross that off the list of possible reason(s) why for now. Next up will be to check the DIP Switches to see what they are set at. That's where I am at until

next time.

=~=~=~=

->In This Week's Gaming Section - Each FF7 Remake Episode: Huge!
Sony Unlocks PS4's Seventh CPU Core!
Kojima Banned From Game Awards!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!

Each Final Fantasy 7 Remake Episode To Be As Big As A 'Full-sized Game'

According to Final Fantasy 7 Remake's Producer Yoshinoro Kitase and Director Tetsuya Nomura, the game is simply too big for a single release. As a result of this, Final Fantasy 7 will be seeing an episodic release, similar to the likes of Telltale games.

This revelation left they community wondering exactly how big FF7 Remake is and how many episodes will be released. Square Enix didn't spare the community any details on this, in fact, they wouldn't even hint at how long fans would have to wait between episode releases.

However, Square did clarify something to Kotaku:

"It means instead of concluding in one entry, multiple entries are being considered in development. Each entry will have its own unique story. As a gaming experience, each entry will have the volume of content equal to a full-sized game."

It's not the most detailed oriented statement, but at least it offers a little more context. It's interesting to note that Square Enix decided to take the episodic approach to the new Hitman game as a digitally released episodic game. When the story arc for Hitman releases, a physical version will be released.

I wonder if the two games will share a similar nature.

Sony Unlocks PS4's Seventh CPU Core

Sony is giving developers further access to the PlayStation 4’s CPU resources, potentially paving the way for enhanced performance in future games, if the latest documentation from a middleware company is to be believed.

Buried within the most recent update details for the audio tool FMOD, which was released mid-November, a note reads: "PS4-Added FMOD_THREAD_CORE6 to allow access to the newly unlocked 7th core."

The data, which was unearthed on the Beyond3D developer forum, has become the subject of speculation across numerous online game communities such as NeoGAF.

Unless it was written in error, FMOD’s note suggests that Sony has made a crucial back-end change to the PS4 system software that, in theory, allows the platform’s games to draw from further processor resources.

The PS4 is assembled with an eight-core AMD Jaguar, clocked at 1.6GHz. Two of those cores are reserved for system operations, along with about 3.5GB of its memory. In January, Microsoft began to allow developers to use the Xbox One’s seventh CPU core, at least partially, which is believed to be one explanation for the enhanced performance of games released in 2015 compared to the year prior.

Differences between PS4 and Xbox One resolution and frame-rates have been less pronounced in 2015, with often no meaningful difference between both systems, as some examples below demonstrate:

    Battlefield Hardline: PS4 900p, Xbox One 720p
    Star Wars Battlefront: PS4 900p, Xbox One 720p
    Batman Arkham Knight: PS4 1080p, Xbox One 900p
    Metal Gear Solid 5: PS4 1080p, Xbox One 900p
    Call of Duty: Black Ops 3: PS4 1080p, Xbox One 1080p-900p (dynamic)
    Project CARS: PS4 1080p, Xbox One 900p
    Evolve: PS4 1080p, Xbox One 900p

Whether the enhanced CPU access on PS4 could result in a widening of that gap is a matter for debate.

Konami Bans Metal Gear Solid 5 Creator Kojima From Game Awards

Metal Gear Solid creator Hideo Kojima was instructed he was not permitted to attend The Game Awards 2015 ceremony to accept any awards for Metal Gear Solid V: The Phantom Pain, host Geoff Keighley has revealed.

As you noticed Hideo Kojima is not here with us tonight and I want to tell you a little bit about that, explained Keighley.
Mr. Kojima had every intention of being with us tonight but unfortunately he was informed by a lawyer representing Konami just recently that he would not be allowed to travel to tonight s awards ceremony to accept any awards.

He s still under an employment contract and it s disappointing,

and it s inconceivable to me that an artist like Hideo would not be allowed to come here and celebrate with his peers and his fellow teammates.

Metal Gear Solid V won best action/adventure game during the show. The award was accepted on behalf of Kojima and the Kojima Productions team by Kiefer Sutherland, voice of Snake in MGSV.

It was reported in October that Hideo Kojima had finally parted ways with Konami after a long-running saga between the two, although Konami officially denied Kojima had left, insisting Kojima remained listed as a company employee.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

France Looking at Banning Tor, Blocking Public Wi-Fi

According to leaked documents France's Ministry of Interior is considering two new proposals: a ban on free and shared Wi-Fi connections during a state of emergency, and measures to block Tor being used inside France.

The documents were seen by the French newspaper Le Monde. According to the paper, new bills could be presented to parliament as soon as January 2016. These proposals are presumably in response to the attacks in Paris last month where 130 people were murdered.

The first proposal, according to Le Monde, would forbid free and shared Wi-Fi during a state of emergency. The new measure is justified by way of a police opinion, saying that it's tough to track people who use public hotspots.

The second proposal is a little more gnarly: the Ministry of Interior is looking at blocking and/or forbidding the use of Tor completely. Blocking people from using Tor within France is technologically quite complex, but the French government could definitely make it difficult for the average user to find and connect to the Tor network. If the French government needs some help in getting their blockade set up, they could always talk to the only other country in the world known to successfully block Tor: China, with its Great Firewall.

Forbidding the use of Tor through legislative means is another option: France could simply make it illegal for people to access Tor. The difficulty there, though, is in the policing of that new law: the country's ISPs would have to snoop on its users to find out who is using Tor, and then report back to the police. In the UK, where the new Snooper's Charter may require ISPs to log the last 12 months of user activity, a lot of resistance is being met.

The main problem with such a ban on Tor is that it wouldn’t achieve a whole lot. Would-be terrorists could still access Tor from outside the country, and if they manage to access Tor from within France I doubt they’re concerned about being arrested for illegal use of the network. There is evidence to suggest that the recent Paris attacks were planned via unencrypted channels, too: the Bataclan "go" message was sent in the clear via SMS.

On the other hand, criminalising and/or blocking Tor might affect many other legitimate users of the network, such as whistleblowers, journalists, and anyone else who wants to surf the Web privately.

The proposal to block Wi-Fi hotspots during a state of emergency is slightly more feasible, and you can see where the French government is coming from but again, it would be technologically very difficult to implement, and the collateral damage would be huge. Millions of people would have to go without public Wi-Fi access, potentially for weeks at a time.

On November 20, a week after the attacks in Paris, France introduced new legislation that extended the current state of emergency to three months. At the same time, new laws were also introduced to make it easier for the Minister of the Interior to block any terrorism-related website, and to dramatically increase police powers for searching seized devices. The French prime minister suggested that they may soon make it illegal to merely visit a terrorism-related website, too.

Come January 2016 we’ll see if the French government actually goes ahead with these new Tor and Wi-Fi blocking measures. Hopefully cooler heads will prevail: France is one of the most powerful and influential Western democracies, but it’s also rapidly becoming one of the most illiberal. If France rolls out its own Great Firewall, it would then be whole lot easier for the UK, Germany, and other neighbouring countries to do the same thing.

Anonymous Celebrates ISIS Trolling Day

If you ve been looking for your chance to make fun of ISIS, now s the time.

Social media sites are abuzz on Friday with users targeting the Islamic State, better known as ISIS or ISIL. Web users around the globe are posting images and videos poking fun at ISIS. A surprisingly large number of people have edited images of the militant group s members, replacing their faces with ducks. The hashtags #ISISTrollingDay, #trollingday, and #Daeshbags have also gone viral. The #Daeshbags hashtag is a reference to the term Daesh, another name for ISIS that the militant group reportedly views as derogatory.

The social media posts are part of what hacking collective Anonymous calls ISIS Trolling Day. Earlier this week, Anonymous, which has claimed to have taken down hundreds of social media

accounts attributed to ISIS as part of its cyber war against the militant group, called on all Internet users to join its members in ISIS Trolling Day.

We ask you to show your support and help against ISIS by joining us and trolling them, the hacking collective wrote on file-sharing website Ghostbin. Do not think you have to be part of Anonymous, anyone can do this and does not require special skills.

Anonymous added that it wanted users to take to Facebook, Twitter, Instagram, YouTube, and anywhere else in the real world to troll ISIS.

Trolling is an Internet term used to define abusive or sometimes-threatening comments. Trolls, as they re called, often use inflammatory language on forums and comment areas, but have in recent years set up shop on social media.

While it s unlikely that ISIS Trolling Day will do much to disrupt the militant group s plans, it represents an important show of solidarity against ISIS.

ISIS has claimed responsibility for two tragic attacks in Paris and San Bernardino in the last two months. Anonymous declared cyber war against ISIS after the Paris attacks. Meanwhile, ISIS, which called Anonymous idiots, has used social media to celebrate the attacks.

Indeed, ISIS has an extremely sophisticated digital apparatus it uses to recruit new members and share propaganda. ISIS uses social media, as well video-sharing sites like YouTube, to spread its content. While those companies have worked to remove those accounts and scrub ISIS from their services, the militant group is still active online. The militant group has its own smartphone app and uses encrypted messaging service Telegram to communicate.

Lawmakers, including President Obama, as well as major technology executives, like Eric Schmidt, say that more work needs to be done to fight terrorist activity online. Schmidt said in an op-ed in The New York Times earlier this week that the best way forward would be for governments, tech companies, and Internet users to come together and find ways to safeguard the web against hate and harassment.

For now, no solutions have been presented. Still, ISIS Trolling Day aims at getting more people invested in combating ISIS online. And at least so far, it seems to be working.

Someone Just Tried to Take Down Internet’s Backbone With 5 Million Queries/Sec

Someone just DDoSed one of the most critical organs of the Internet anatomy The Internet’s DNS Root Servers.

Early last week, a flood of as many as 5 Million queries per

second hit many of the Internet’s DNS (Domain Name System) Root Servers that act as the authoritative reference for mapping domain names to IP addresses and are a total of 13 in numbers.

The attack, commonly known as Distributed Denial of Service (DDoS) attack, took place on two separate occasions.

The first DDoS attack to the Internet’s backbone root servers launched on November 30 that lasted 160 minutes (almost 3 hours), and the second one started on December 1 that lasted almost an hour.

The DDoS attack was able to knock 3 out of the 13 DNS root servers of the Internet offline for a couple of hours.

The request queries fired at the servers were valid DNS messages addressed towards a single domain name in the first DDoS attack, and the second day’s DDoS attack addressed towards a different domain name.

According to the analysis published by the root server operators on Tuesday, each attack fired up to 5 million queries/second per DNS root name server that was enough to flood the network and cause timeouts on the B, C, G, and H root servers.

There is no indication of who or what was behind the large-scale DDoS attacks because the source IP addresses used in the attacks were very well distributed and randomized across the entire IPv4 address space.

However, the DDoS attacks did not cause any serious damage to the Internet, but a mere delay for some of the Internet users who made DNS queries through their web browser, FTP, SSH, or other clients.

The motive for such attacks is still unclear because disabling or knocking down a root server won’t have a severe impact on the Internet as there are several thousand of other DNS servers managing DNS queries.

"The DNS Root Name Server system functioned as [it’s] designed, demonstrating overall robustness in the face of [massive] traffic floods observed at numerous DNS Root Name Servers," Root Server Operators says (PDF), referring to the backup system employed by DNS servers.

Like the Internet, DNS is constructed on a mesh-like structure, so if one server doesn’t respond to a request, other servers step in and provide a DNS query result.

According to the DNS root server operators, the attack was not the result of a reflective DDoS attack in which open and misconfigured DNS is used to launch high-bandwidth DDoS attacks on the target.

Despite all the facts, any attack on the critical infrastructure of the Internet is taken extremely seriously.

The DNS root server operators recommended the Internet Service Providers (ISPs) to implement Source Address Validation and

BCP 38, an Internet Engineering Task Force standard that helps defeat IP address spoofing.

At School And At Home, How Much Does The Internet Know About Kids?

Children’s personal information isn’t supposed to be an online commodity. But whether kids are using Google apps at school or Internet-connected toys at home, they’re generating a stream of data about themselves. And some advocates say that information can be collected too easily and sometimes, protected too poorly.

Last month, a hacker stole personal information and photos of more than six million children after breaking into the computer records of a educational toy company, VTech.

VTech says that they’ve since hired a security company to deal with the breach. That might not be enough to convince Congress Sen. Ed Markey (D-Mass.) and Rep. Joe Barton (R-Texas) sent a letter to VTech, wanting to know if the company is complying with a law called the Children’s Online Privacy Protection Act.

The issue, of course, spans beyond VTech. In the toy world, there’s the new Internet-connected Barbie doll, which has also been found to have security flaws, for example. And privacy advocates have long waged a battle against cookies and other data collection based on kids’ Internet activity.

Google is one of the companies that have come under fire. A nonprofit advocacy group called Electronic Frontier Foundation has filed a complaint with the Federal Trade Commission over Google’s data mining practices. More than half of classroom computers in the U.S. are Chromebooks and many students and teachers are using Google Apps For Education, a group of tools that include Gmail, Google Calendar, Google Docs and the purpose-built Google Classroom.

Anya Kamenetz of NPR’s Ed Team and Lorenzo Franceschi-Bicchierai, a staff writer for the tech news website Motherboard who has reported on the VTech data hack, spoke to All Things Considered about the issue of children’s privacy. Here are a few takeaways.

LORENZO FRANCESCHI-BICCHIERAI

On the VTech hacker’s motivation

He realized their services were really easy to break into. And he just took a peek in and found there was a lot of personal data and he was like, whoa, I should not be able to get this.

On what the hacker discovered

He analyzed it (the data) a little bit further, and he realized that you could actually link the two databases, and basically figure out who the kids were. The children database only had their first names, so you couldn’t really identify the children because you only had Mike, Lucy, Sarah, whatever. But from some other data in the files, Troy Hunt (an Internet security analyst)

realized that you could actually link the two databases and figure out who the kids were, who were their parents, and effectively find where the kids lived and all this creepy information.

On sharing addresses with toy companies

If you're a parent and you buy a V-Tech toy, put in a fake address. If the company doesn't need that address, you might want to not give it out. And that way, there's no damage there.

On planning for the future

The big takeaway here is that these things can happen, and as we connect more stuff to the Internet, we're going to lose data. That's unfortunate but that's the reality. So we have to accept it and find ways to limit the damage if it happens — and also, hold more companies accountable as well.

ANYA KAMENETZ

On what happens when you type a search into Google

When you or I are logged in to Google, whether we're using search, or Maps, or gmail, we have one account and that's following us around — sometimes literally in the physical world — and it's collecting information. When you're logged in and using Chrome, which is their web browser, Google can actually, with permission, track your entire browsing history, every site you visit. And Google uses all this data to better target ads and search results and to improve its services, not only for you but for everyone.

On why that can pose a problem in schools

For students, the rules are supposed to be a little bit different. When students are using the Google Apps for Education and "Core Services" within them — gmail, docs, sheets, slides — Google says that they don't collect personal data to target ads. In fact, they stopped collecting student data for ad-targeting last year after a California lawsuit questioned that practice.

But the EFF says that there's a little bit of a sliding door, a back door: when students are logged into their student Google accounts but they're using other Google services like YouTube videos or they're searching Maps — that Google is collecting that information after all. And when students are using Chrome on these school-issued computers, they're browsing the web and Google potentially has access to their entire browsing history as well.

On legal implications of such data collection

Well, that depends on who you ask. Google denies any wrongdoing here. They have signed a voluntary but binding pledge called the Student Privacy Pledge, along with 200 other companies. And that pledge says that Google will seek parental authorization before collecting data that isn't being used explicitly for educational purposes. And EFF told me that they're not necessarily digging into what Google is doing with this information, they just want Google to get permission.

Patent Troll 66 Big Companies Sued For Using HTTPS Encryption

Are you Using HTTPS on your Website to securely encrypt traffic?

Well, we'll see you in the court.

At least, that's what CryptoPeak is saying to all big brands that utilize HTTPS on their web servers.

Texas-based company CryptoPeak Solutions LLC has filed 66 lawsuits against many big businesses in the US, claiming they have illegally used its patented encryption method Elliptic Curve Cryptography (ECC) on their HTTPS websites.

Elliptic Curve Cryptography (ECC) is a key exchange algorithm that is most widely used on websites secured with Transport Layer Security (TLS) to determine what symmetric keys are used during a session.

Encryption is on the rise after Edward Snowden made the world aware of government s global surveillance programs. Today, many big tech and online services are using encryption to:

- Protect the data transmitted to/from visitor to domain
- Lessen the risk of hacking

However, websites using the ECC key are now at risk of being forced to court for using the protocol. As CryptoPeak snapped up the Patent (US Patent 6,202,150) that describes "Auto-Escrowable and Auto-Certifiable Cryptosystems," which the firm argues covers elliptic curve cryptography (ECC).

The abstract of the US Patent 6,202,150 describes the invention, which was granted in 2001:
patent-troll

Some of the biggest names CryptoPeak Solutions sued include:

- Yahoo
- Netflix
- Pinterest
- AT&T
- Sony
- Groupon
- GoPro
- Etsy
- Petco
- Target
- Costco
- Home Depot
- Expedia
- Barnes & Noble
- Multiple financial institutions and hotel chains

"Defendant has committed direct infringement by its actions that comprise using one or more sites that utilize Elliptic Curve

Cryptography Cipher Suites for the Transport Layer Security (TLS) protocol (the Accused Instrumentalities)," according to the lawsuits.

CryptoPeak can easily be categorized as a "Patent Troll," as it is still unclear if the cases will be successful or not. Since the patent describes some of the key tenets of ECC, which includes generating and publishing of public keys, not obvious corresponds directly to its implementation in HTTPS connections.

Some companies targeted by the firm are fighting the lawsuit that seeks damages and royalties, and other like Scottrade are doing out of court settlements, saying "all matters in controversy between CryptoPeak and Scottrade have been settled, in principle."

Netflix, one of over 60 companies being dragged to court, called CryptoKey’s lawsuit "invalid" from the outset and filed a case to be dismissed under FED.

"The defect in these claims is so glaring that CryptoPeak s only choice is to request that the court overlooks the express words of the claims, construe the claims to read out certain language, or even correct the claims," Netflix said in a court filing.

Now, let’s see what happens next.

Microsoft Sets Record With 135 Security Bulletins Issued in 2015

Microsoft released 12 security bulletins for the last Patch Tuesday update of 2015, resolving a total of 71 vulnerabilities. Importantly, nine of the bulletins are rated as critical, including a zero-day flaw that hackers could use to pull off an escalation of privilege exploit.

The critical updates affect multiple components, including the VBScript and JScript engine, the Windows DNS server, .Net, Microsoft Office, Skype for Business, Microsoft Lync and Silverlight. Three of the updates also affect browsers, namely Internet Explorer and Microsoft Edge, while a significant number also impact the Windows operating system.

The latest Patch Tuesday brings up the total tally of bulletins for the year to 135, which is a significant increase from the average of recent years, noted Wolfgang Kandek, the CTO of Qualys, in a blog post.

"New products by Microsoft only explain a small part of this increase, for example the new Edge browser only added five bulletins of its own this year," explained Kandek. "The majority of the increase is due to new parts of the Windows ecosystem that are being investigated for the first time, a tendency that shows how much more important computer security has become over the years."

Ultimately, the high number of critical updates means that businesses will need to get affected systems patched as soon as possible. Administrators can expect extra work this week,

considering how Adobe and Google also released their own updates at the same time.

For its part, Adobe released a whopper of an update, resolving 78 vulnerabilities in Flash Player software, while Google also released a security update for its Chrome browser.

PC Sales Will Keep Falling, But Not for Long

A new report suggests that 2016 was a rough year for PC makers with worldwide shipments falling by more than 10%.

PCs have had a tough year, as consumers continue to opt for a new smartphone or tablet over a laptop or desktop computer. According to market researcher IDC, worldwide PC shipments for 2015 will be 10.3% lower than last year. And in the all-important holiday quarter, PC shipments are expected to fall 10%.

It s a discouraging forecast for PC makers, which had hoped on Microsoft s new Windows 10 operating system would encourage people to upgrade their PC. Historically, a new version of Windows has been a strong reason for enterprise and consumers to replace old machines. But Windows 10 is a free upgrade for many systems, and some users are opting to try a software update over replacing their old computers.

The free upgrade to Windows 10 enables some users to postpone an upgrade a little, but not indefinitely, said IDC research VP Loren Loverde in a statement. According to Loverde, some consumers will use the free operating system upgrade to test their transition to Windows 10, but they may discover key features, such as robust touchscreen support, that could induce them to buy a new device.

Despite the substantial shift in spending and usage models from PCs toward tablets and phones in recent years, very few people are giving up on their PC they are just making it last longer, Loverde said.

But when Microsoft ends security updates for Windows 7, the PC world may get a boost from enterprise users upgrading to newer operating systems though that s not expected to happen until 2020.

Another bright spot for the PC market is increasingly sophisticated laptops with touch screens, which IDC predicts will continue to gain share from desktop as well as tablet-first detachables. IDC calls these kind of devices convertibles, and believes they will continue to grow, even factoring the rise of tablets with keyboard accessories that can largely perform the same tasks.

But one key product missing from IDC s forecast is Microsoft s Surface Pro tablet, which runs a full version of Windows and is being marketed as a laptop replacement. IDC doesn t include tablets in its tally, but a separate report suggested that the tablet market would also decline 8% this year, compared to 2014.

However, if IDC were to include detachable tablets such as the Apple iPad Pro in its forecast, it would only boost PC growth by 3 percentage points.

Meanwhile, rival research firm Gartner, which does include tablets in its calculation, largely concurs with IDC s pessimistic forecast, announcing in October that third quarter PC shipments fell 7.7%.

But there may be a light at the end of the tunnel for PC makers. IDC analysts believe sales are expected to stabilize by the end of 2016, with the market only shrinking by 3.1% in 2016, which is good for 268 million laptops and desktops shipped worldwide.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.